AAD Connect setup guide

Contents

Introduction

In this guide you will find a customized configuration of AAD Connect. This setup is done with mostly default and Microsoft recommended settings. This document is part of a set of information about Office 365/Azure AD and SURFnet SURFconext. More information about this can be found on https://wiki.surfnet.nl/display/services/Ways+of+connecting+with+Office+365+and+consequences

The set was created to help SURF institutions decide whether and how they can use SURFconext federated authentication (and related technology like SURFconext Strong Authentication) with Azure AD services, like Office 365."

We have tested this working setup in our own environment and if you have any questions or you need help, feel free to contact us via support@surfconext.nl

This document is created on 11-07-2017 based on the components that are current at this date. The most up-to-date version can be found on https://wiki.surfnet.nl/display/services/Microsoft+Office+365

Step 1: Run the AAD Connect tool

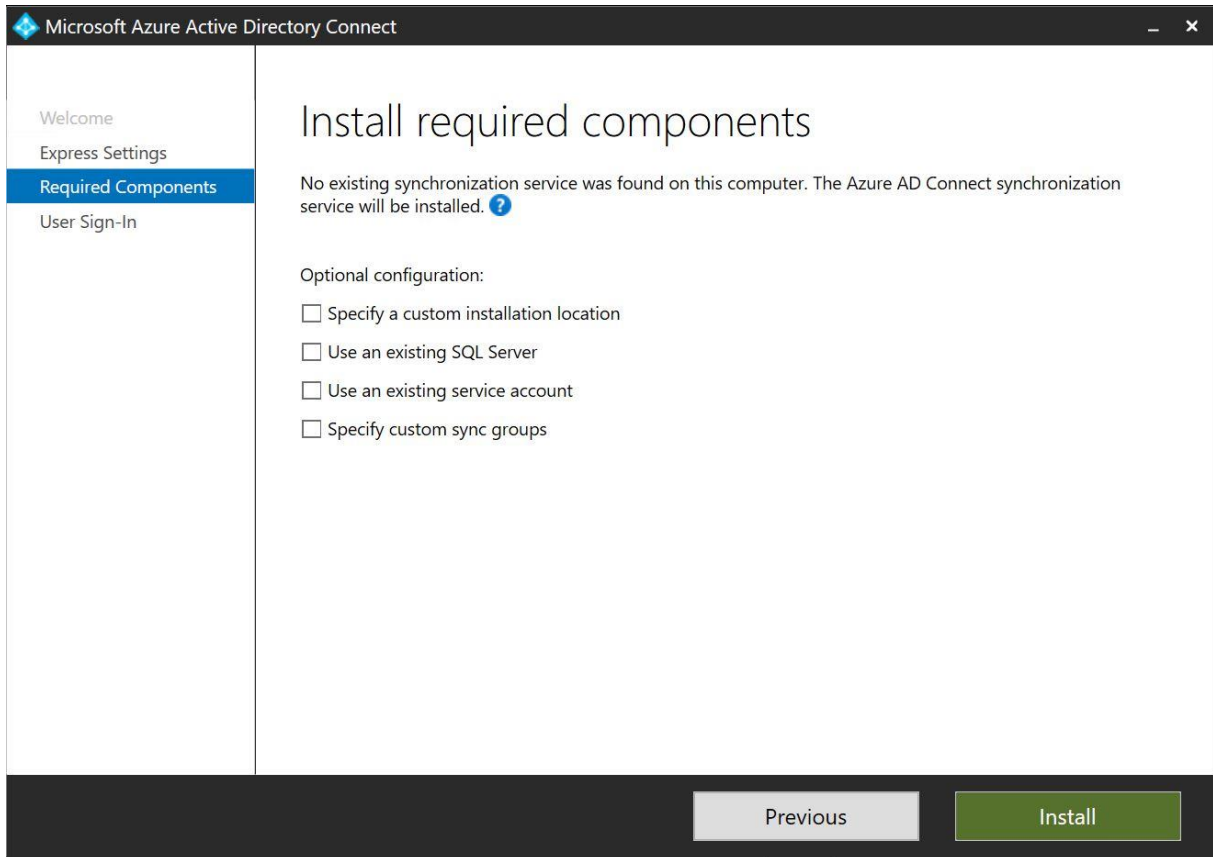Run the AAD Connect tool setup on a server in your domain. The AAD Connect tool can be found here.
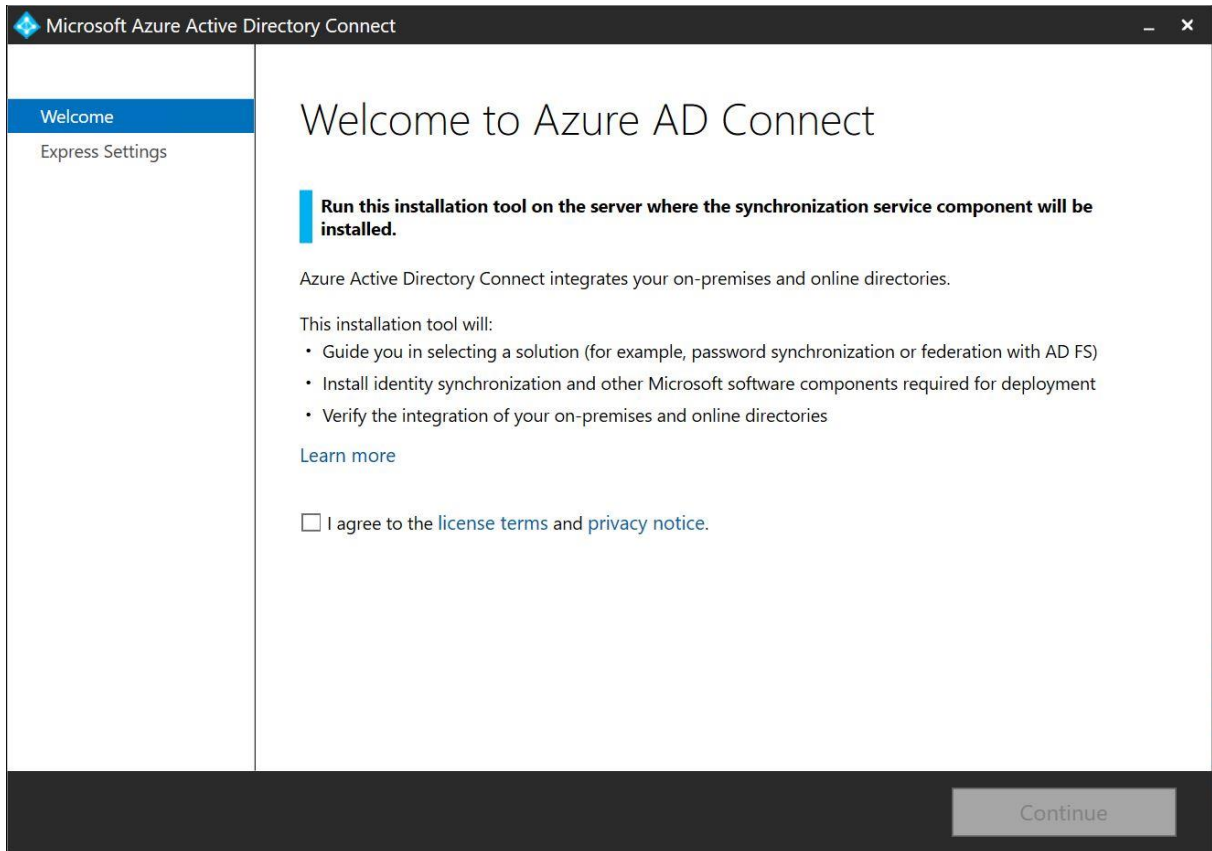
Step 2: Select your setup type

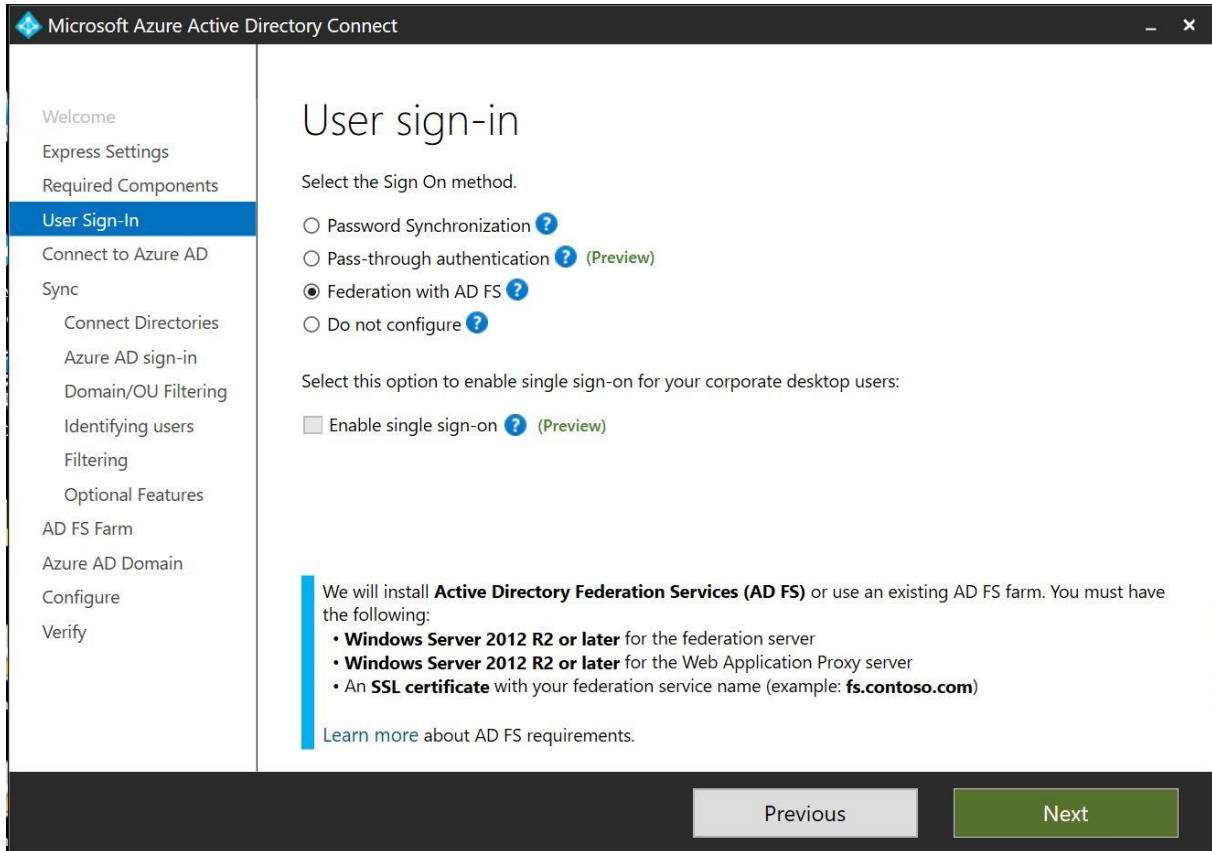You can choose the express settings or to customize your settings. This guide will show you a customized setup.
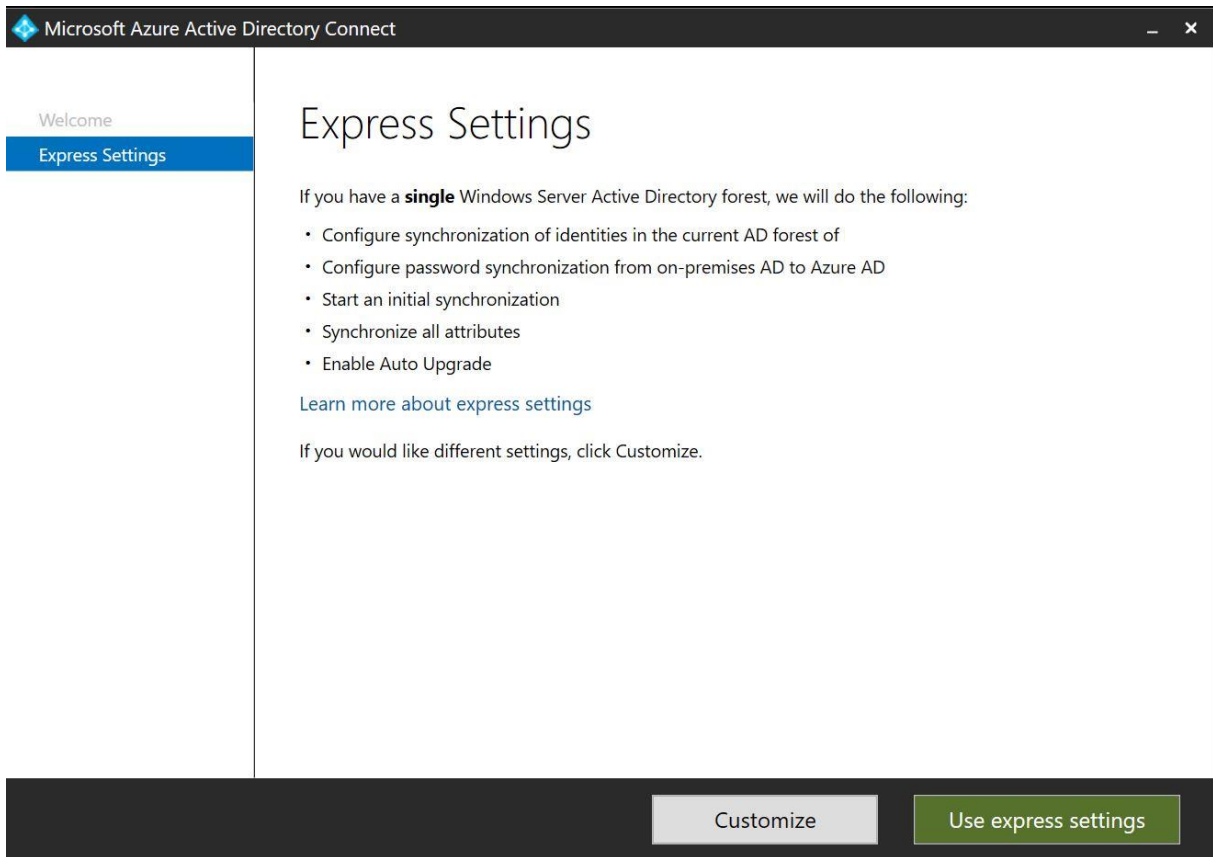
Step 3: Install required components

You can choose your own components in this screen. When you don't select a component, AAD Connect will create them for you. In case you don't use a SQL Server installation, AAD Connect will install SQL Express. When you are working with big numbers of users, then SQL Express is not recommended. We did not add any optional configurations.

Microsoft Azure Active Directory Connect

Install required components

Welcome
Express Settings
Required Components
User Sign-In

No existing synchronization service was found on this computer. The Azure AD Connect synchronization service will be installed. ❓

Optional configuration:
- ☐ Specify a custom installation location
- ☐ Use an existing SQL Server
- ☐ Use an existing service account
- ☐ Specify custom sync groups

Previous   **Install**

Step 4: User Sign-in

In this step you can choose the way users are going to sign in. In this case we are going to choose the 'Federation with AD FS' option. When you select the 'Enable single sign-on' option, you will provide users with domain joined devices to use single sign on.

Step 5: Connect to Azure AD

Fill in your Office 365 tenant admin password to connect to Azure AD

Step 6: Connect your directories

Azure AD Connect will need the forest name to connect with your AD domain services

Step 7: AD Forest account

Azure AD Connect will need an AD Forest account to connect with your AD domain services. If you don't have one, you could let AD connect create one for you.
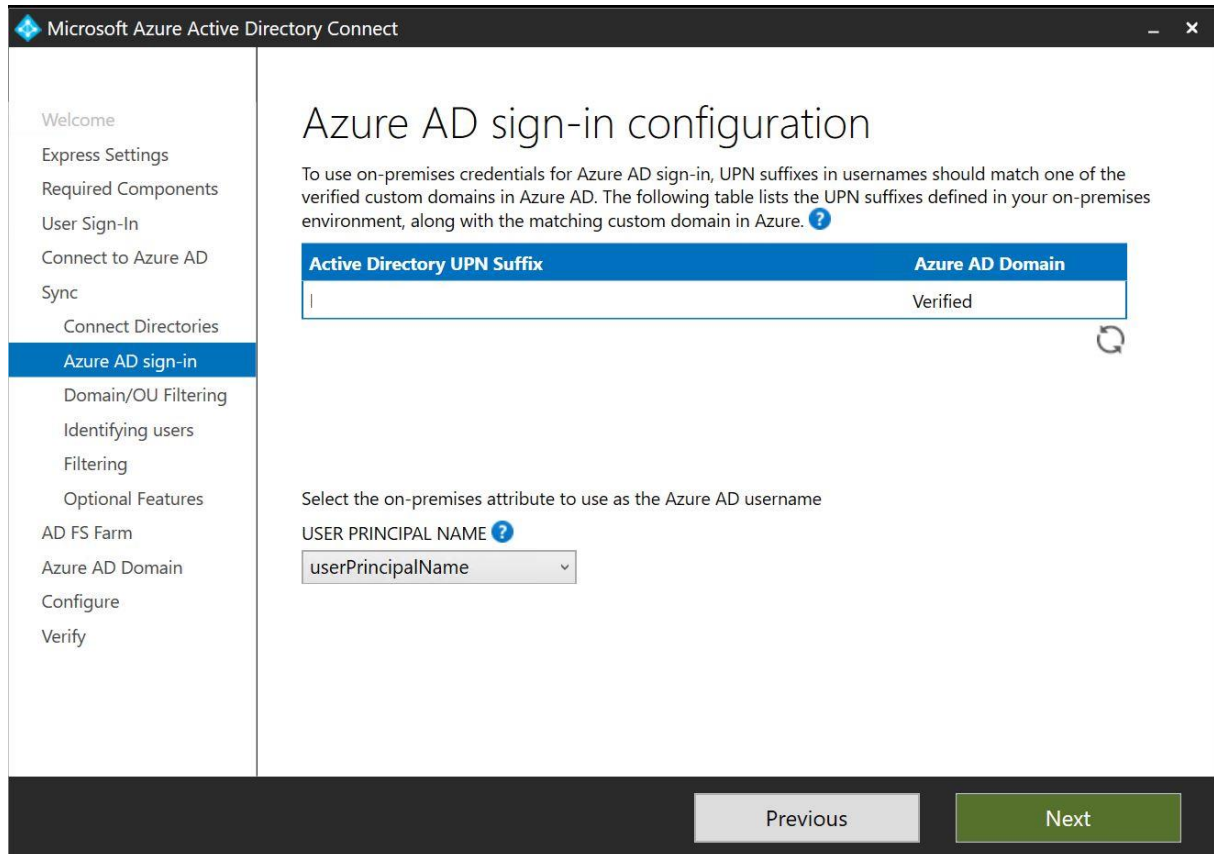
Step 8: Azure AD sign-in configuration

On this page your Office 365 domains will be visible. The verification status will also be visible. In this step, you can choose what AD attribute will be used as User Principal Name. The use of an alternative UPN (such as email), is not supported by every Office 365 application.
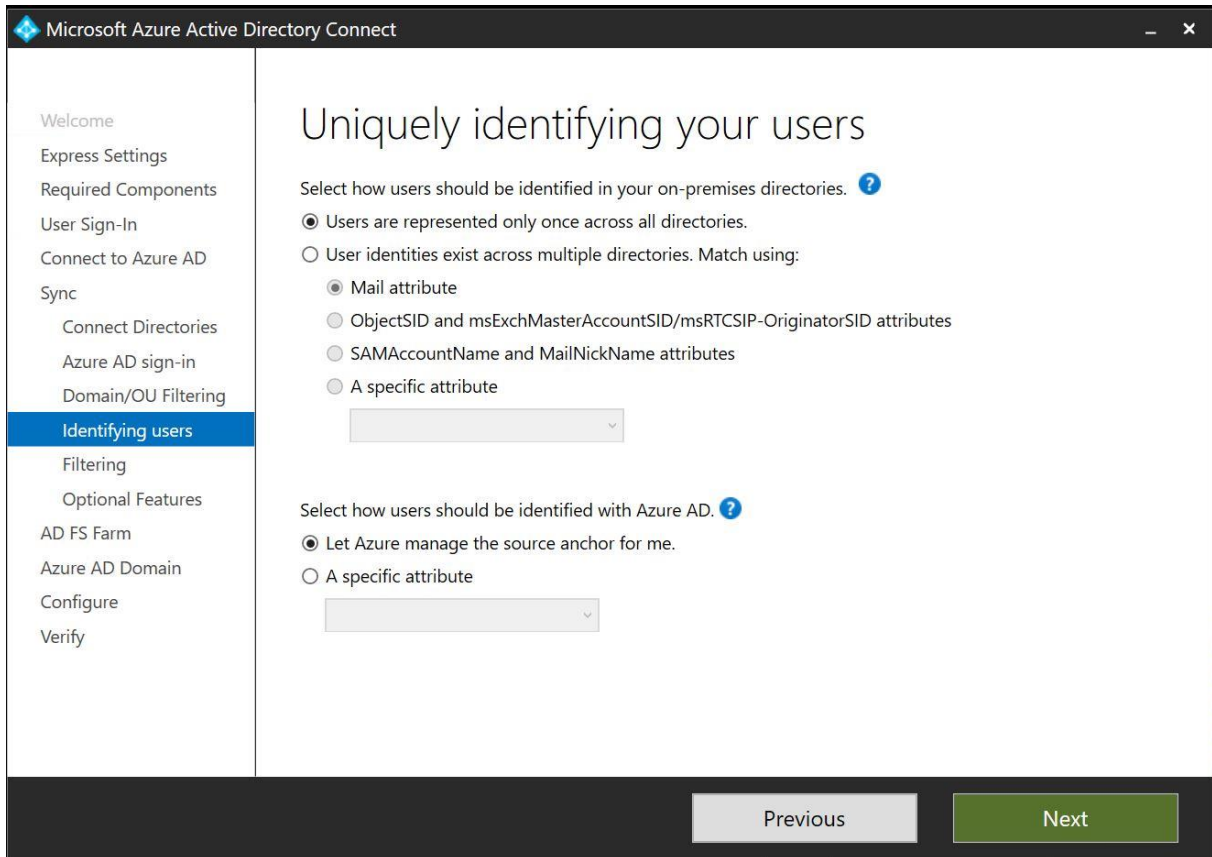
Step 9: Domain and OU filtering

In this step you can select the domains and OU's you would want to sync. By default all domains and OU's are synced.
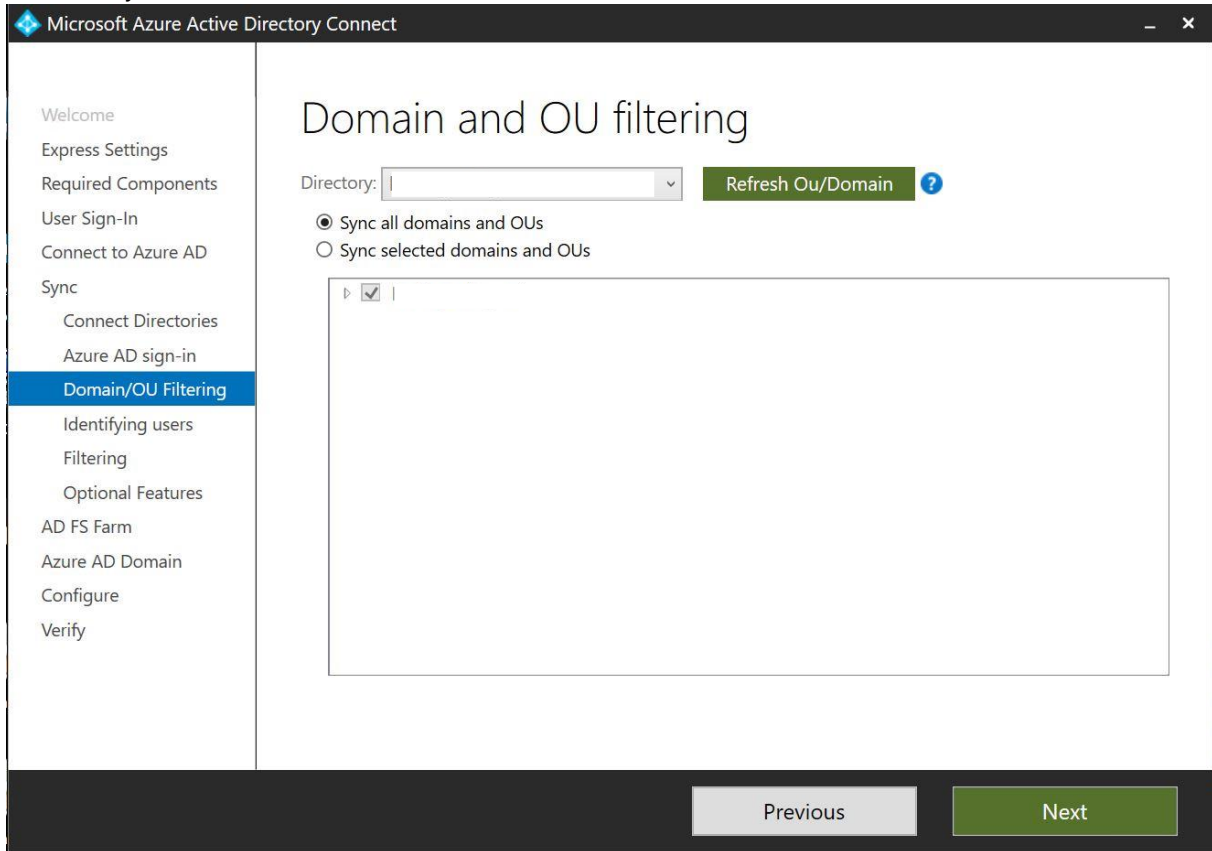
Step 10: Uniquely identifying your users
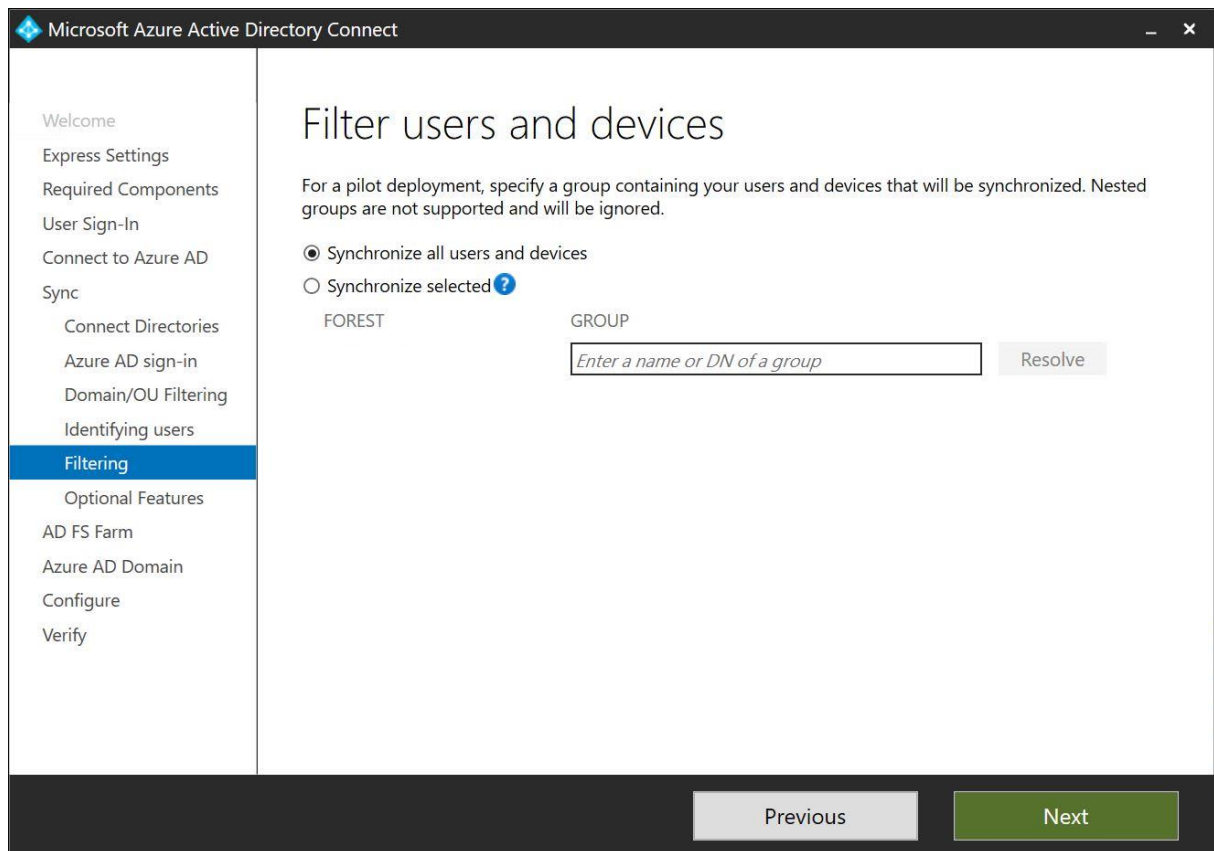
In this step, you can select if users are represented only once across all directories or not. If not, you are able to select an attribute by which the users are identified. You can also select the way users in Azure AD should be identified. You can only set this once for a user! ObjectGUID would be a good attribute to use, or you could just let Azure choose the source anchor for you.

Step 11: Filter users and devices

In this step, you are able to select users and devices that should or should not be synchronized. By default all users and devices are being synced.

Step 12: Optional features

In this step you can select optional features based on your situation. We aren't using the Password synchronization. Also the password writeback isn't enabled because this is not recommended by Microsoft.
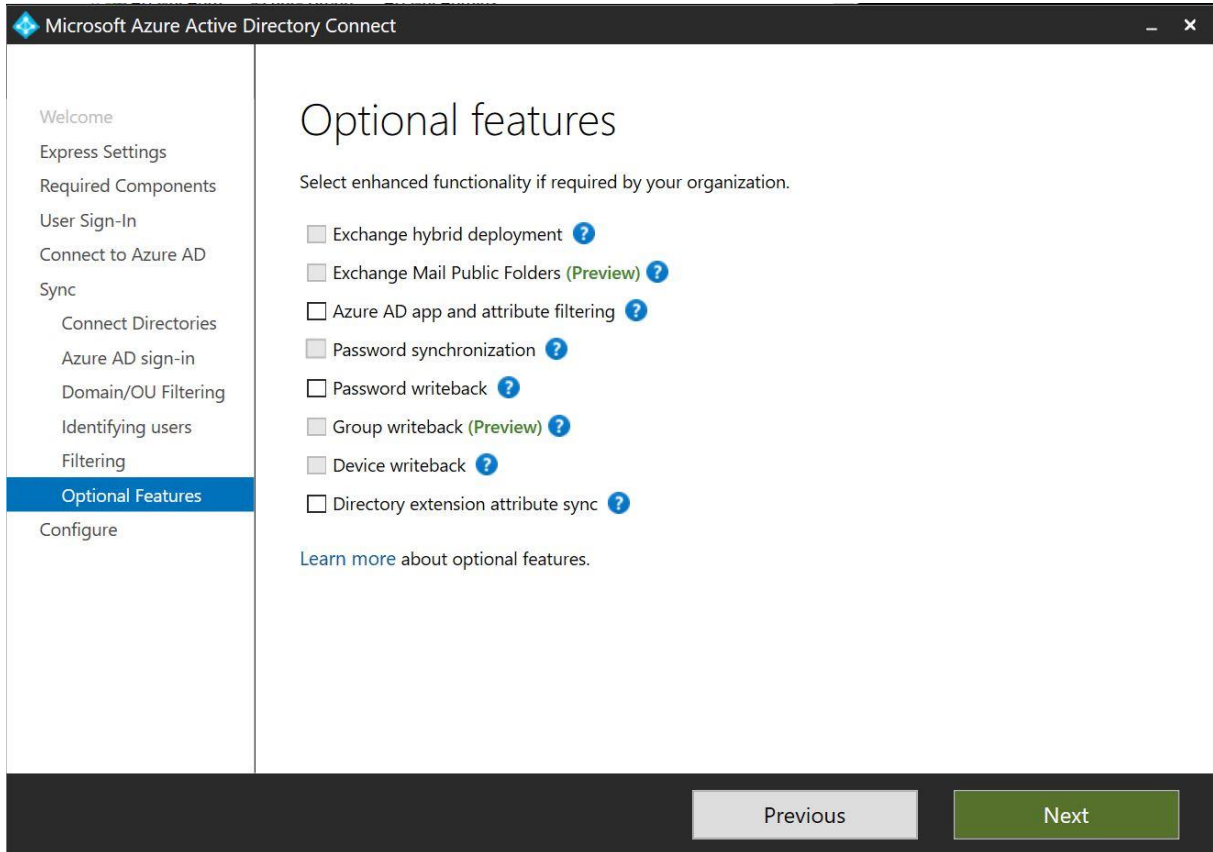
Step 13: AD FS farm

In this step, you can let AAD Connect configure your AD FS farm. You will need a certificate in *.pfx format and fill in the subject name prefix.
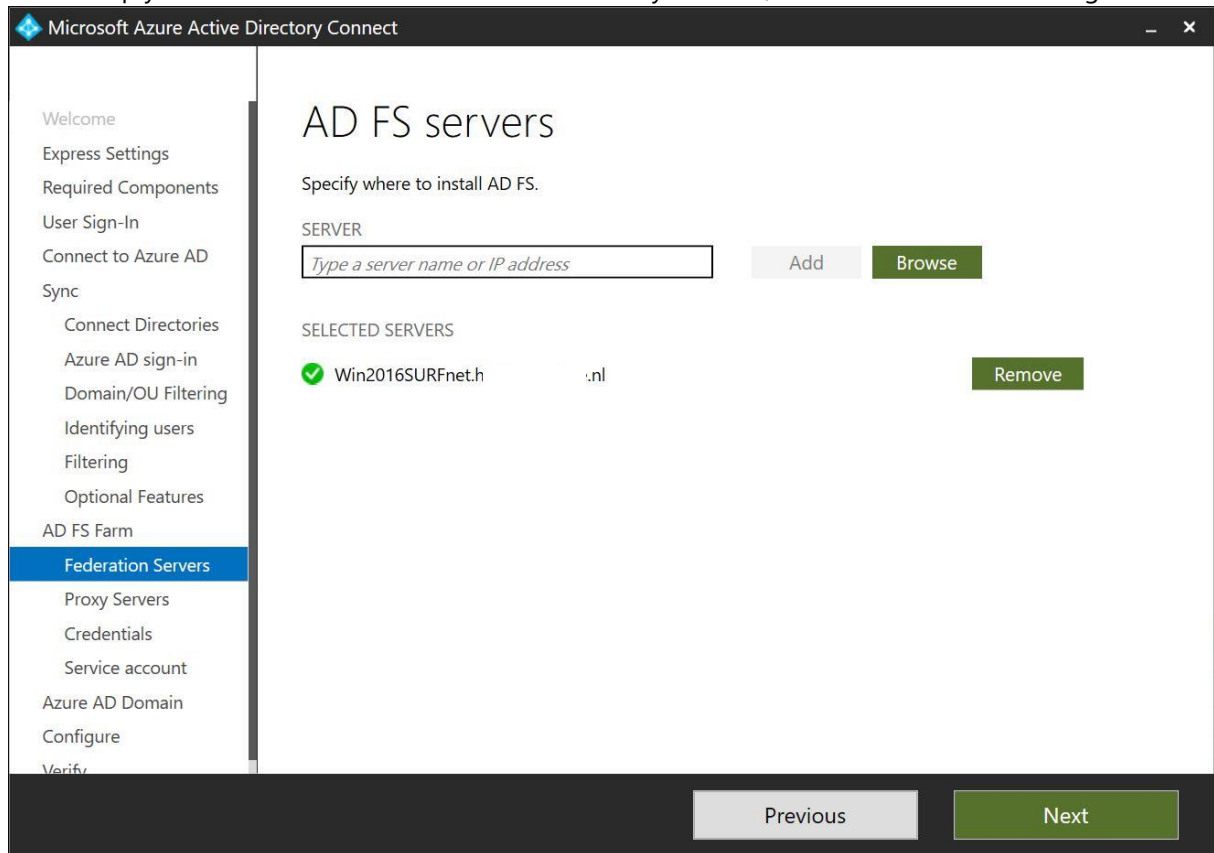
Step 14: AD FS servers

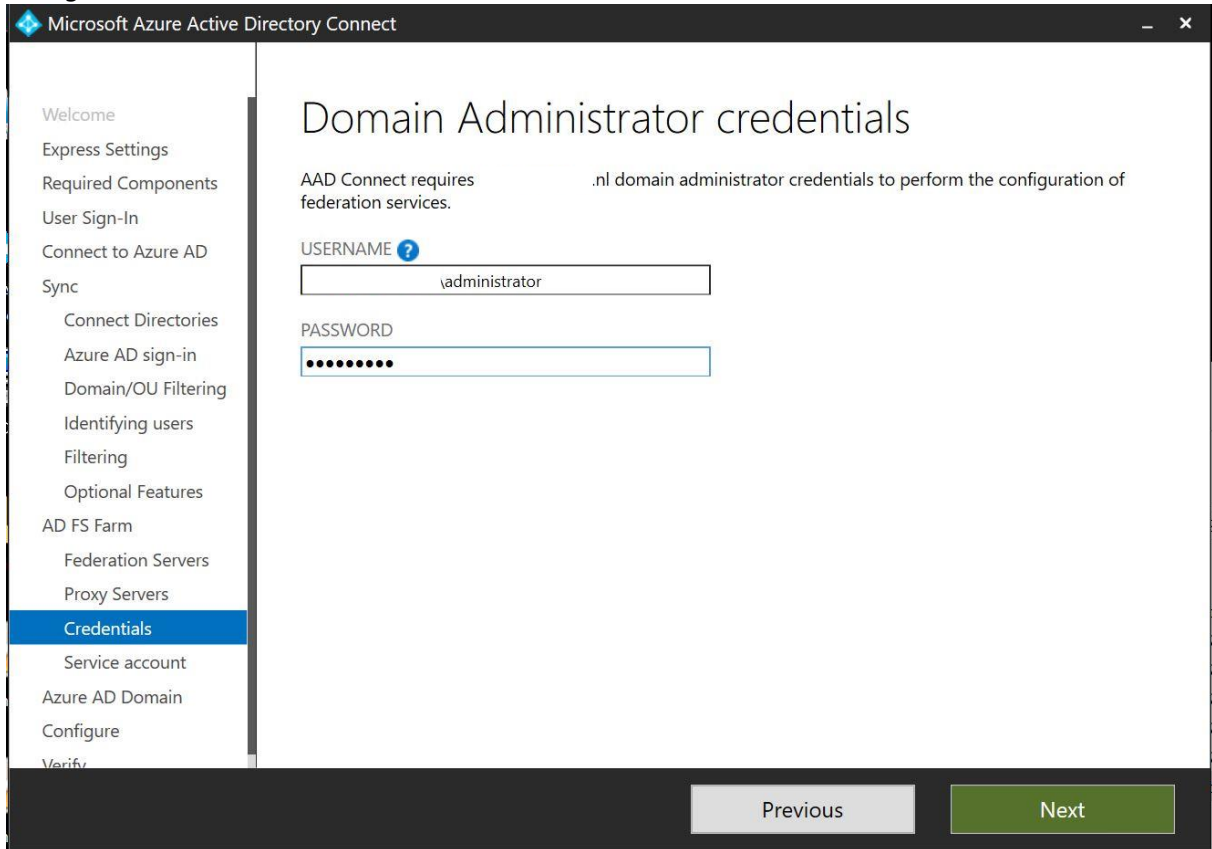In this step you will have to select the AD FS servers in your farm, so AAD Connect can configure them.

Step 15: Web Application Proxy servers

In this step, you will be able to select the Web Applicatons servers in your farm. This is an optional step. We didn't use a Web Application Proxy server.
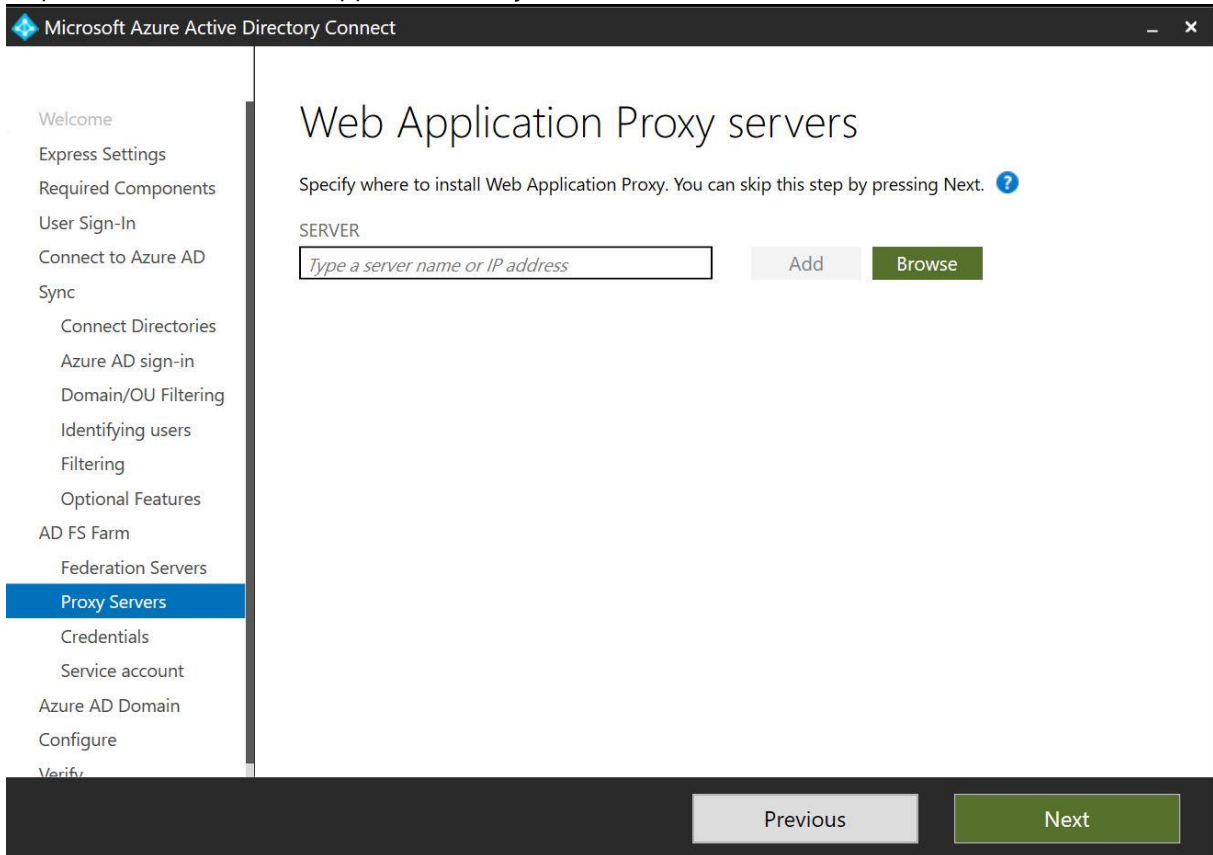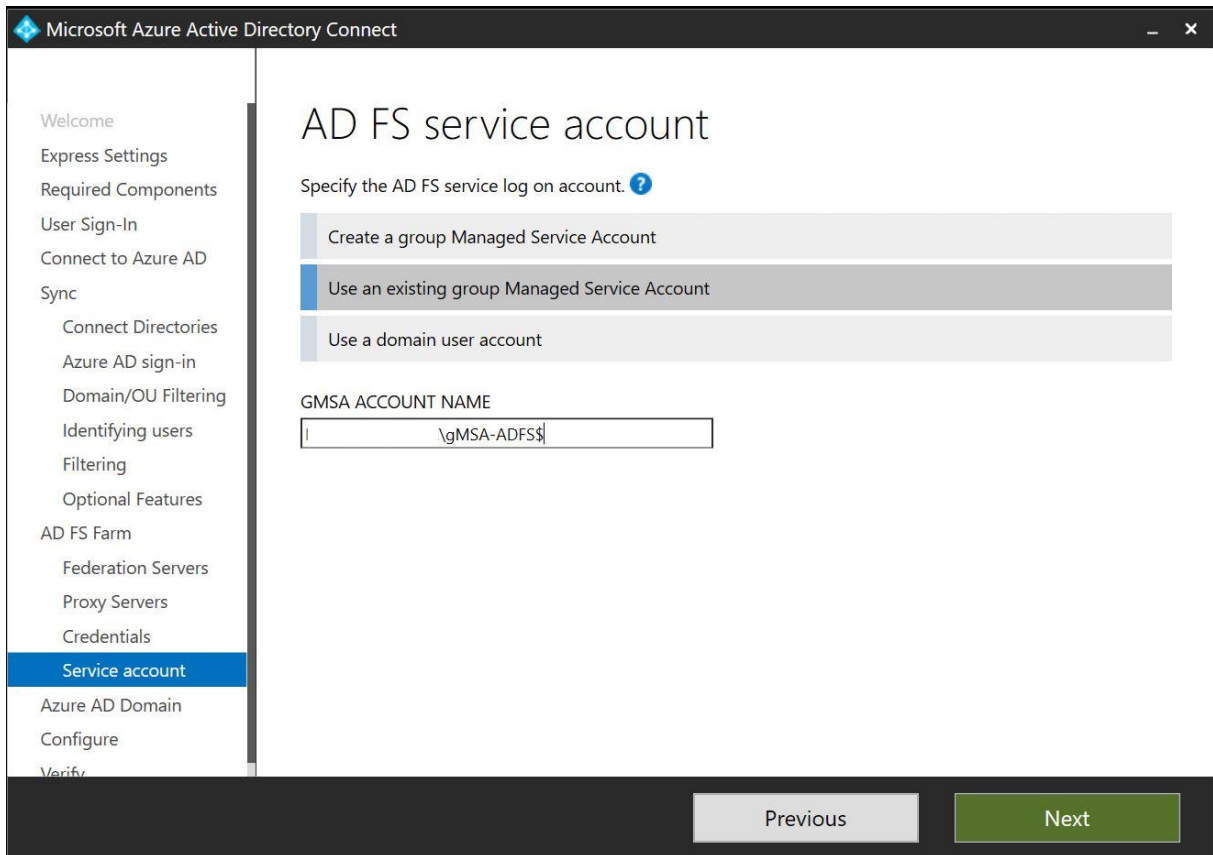
Step 16: Domain Administrator credentials

In this step, you will have to provide the domain administrator credentials to perform the AD FS configuration.

Step 17: AD FS service account

When you are going through the installation step on the [SURFnet wiki](), you've just created a group Managed Service Account. You will have to enter an existing service account, or let AAD Connect create one.

Step 18: Azure AD Domain

You can select the Azure AD Domain you want to federate with your (on-premises) directory. You have to run this step for all domains you want to federate.
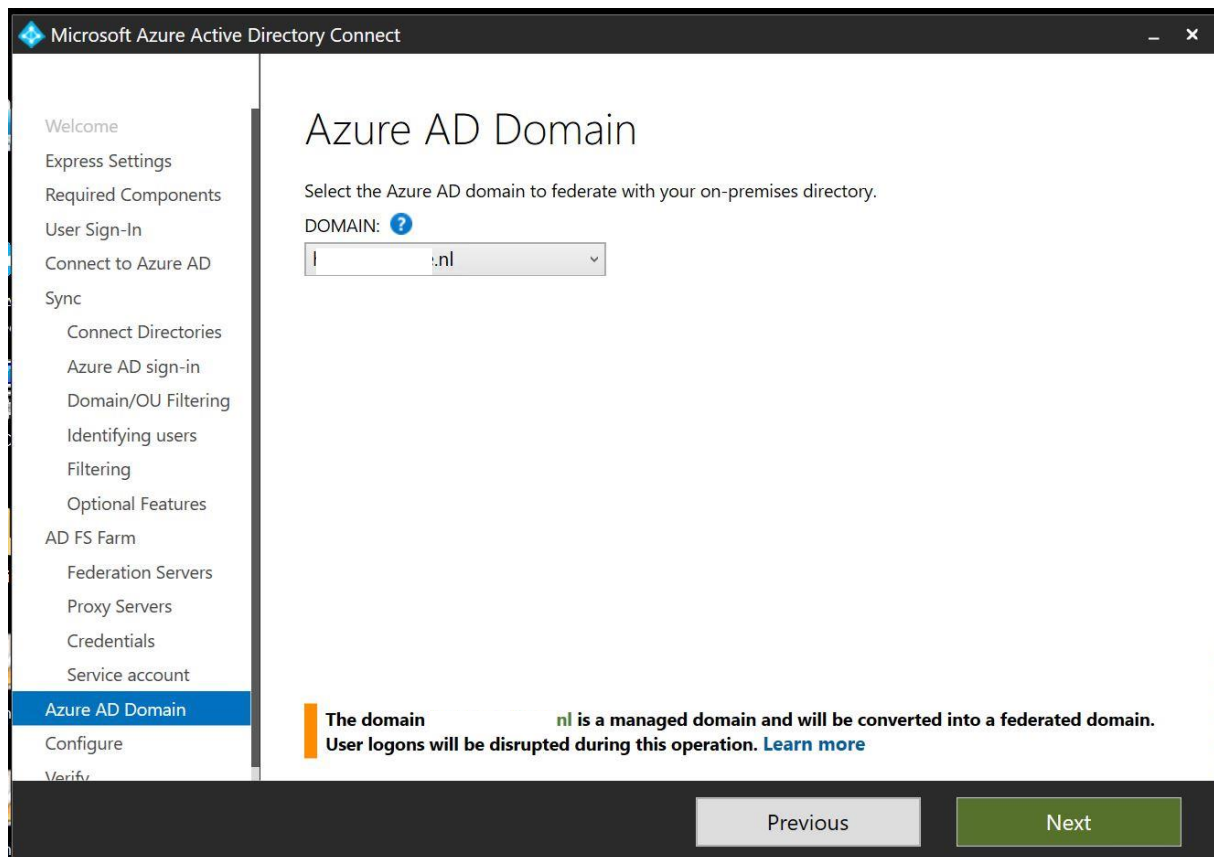
Step 19: Ready to configure

In this step you are able to start the configuration of all of the settings you've selected.
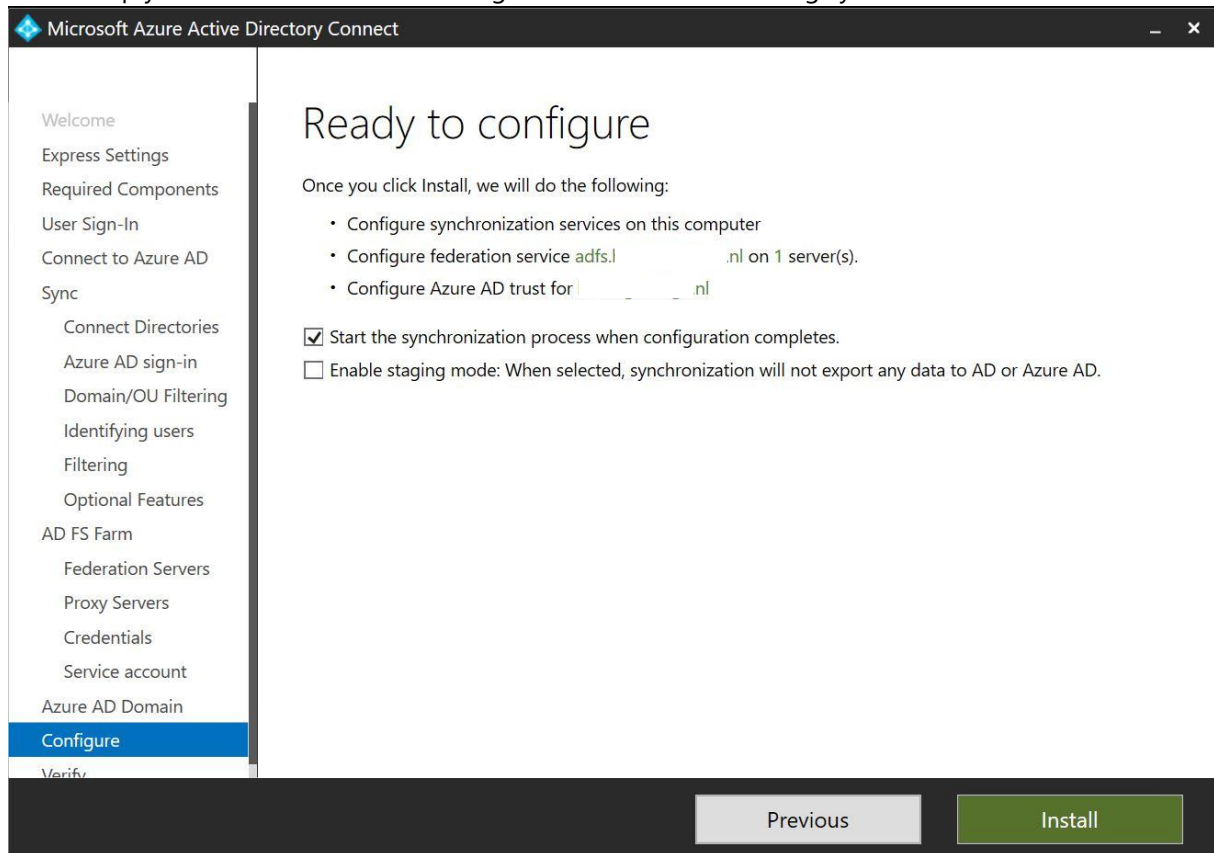
Step 20: Configuration Complete

In this step you will see a summary of completed steps, warnings and errors. In this case it is recommended to enable the AD recycle bin.

Step 21: Verify federation configuration
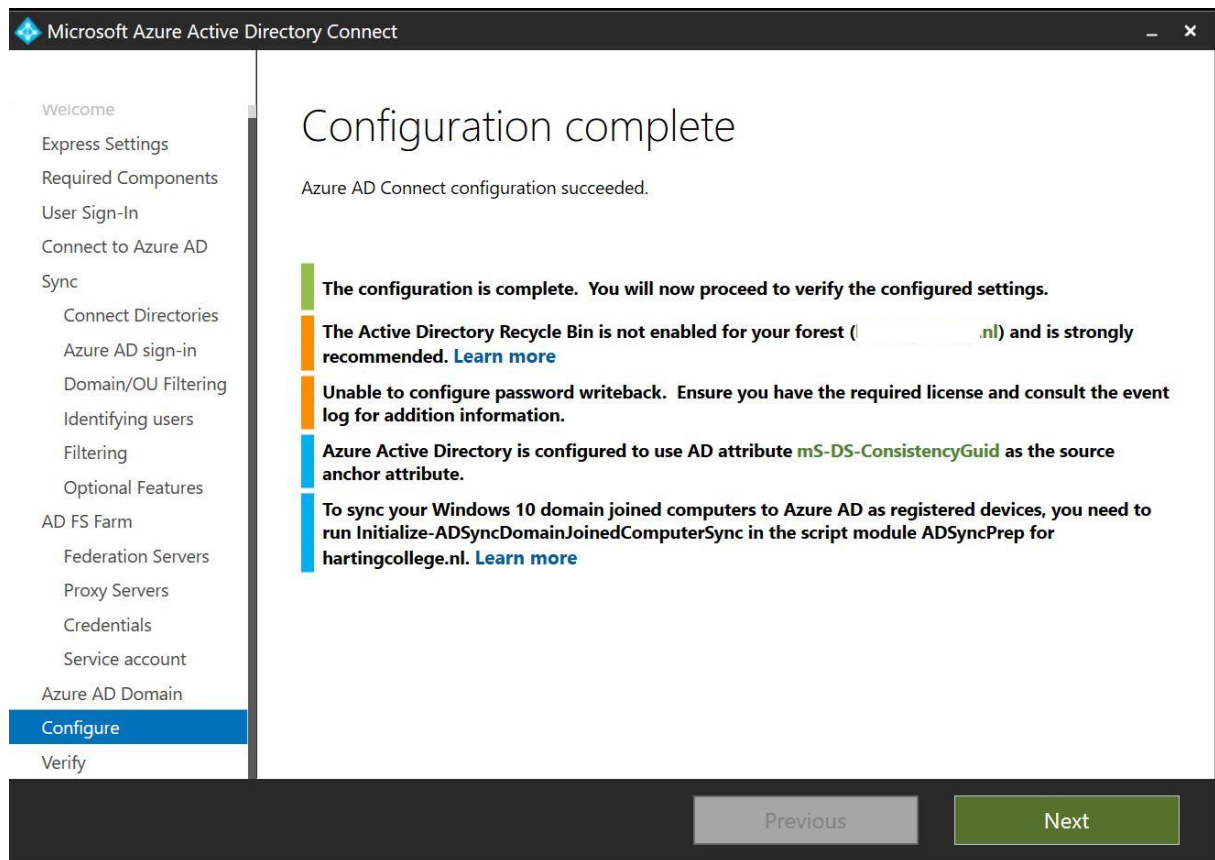
The last step is the verification step for AD FS. If you've created a DNS record for your AD FS server(s), you will be able to test your setup.

Microsoft Azure Active Directory Connect

Verify federation configuration

Federation service configuration succeeded and is ready to verify. Before verification, you must configure domain name resolution for the service.

☐ I have created DNS A records that allow clients to resolve my federation service (adfs.␣␣␣.nl) from the intranet. Extranet verification will not be performed because no Web Application Proxy was configured.

Previous   Verify   Exit